ISO 13491-1:2016-03 (E)

Financial services - Secure cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Abbreviated terms 5

5 Secure cryptographic device concepts 5
5.1 General 5
5.2 Attack scenarios 6
5.2.1 General 6
5.2.2 Penetration 6
5.2.3 Monitoring 6
5.2.4 Manipulation 6
5.2.5 Modification 6
5.2.6 Substitution 6
5.3 Defence measures 7
5.3.1 General 7
5.3.2 Device characteristics 7
5.3.3 Device management 8
5.3.4 Environment 8

6 Requirements for device security characteristics 8
6.1 General 8
6.2 Physical security requirements for SCDs 9
6.2.1 General 9
6.3 Tamper evident requirements 9
6.3.1 General 9
6.4 Tamper resistant requirements 10
6.4.1 General 10
6.5 Tamper responsive requirements 10
6.5.1 General 10
6.6 Logical security requirements for SCDs 11
6.6.1 Dual control 11
6.6.2 Unique key per device 11
6.6.3 Assurance of genuine device 11
6.6.4 Design of functions 11
6.6.5 Use of cryptographic keys 12
6.6.6 Sensitive device states 12
6.6.7 Multiple cryptographic relationships 12
6.6.8 SCD software authentication 12

7 Requirements for device management 12
7.1 General 12
7.2 Life cycle phases 13
7.3 Life cycle protection requirements 14

7.3.1 General 14
7.3.2 Manufacturing phase 14
7.3.3 Post-manufacturing phase 15
7.3.4 Commissioning (initial financial key loading) phase 15
7.3.5 Inactive operational phase 15
7.3.6 Active operational phase (use) 16
7.3.7 Decommissioning (post-use) phase 16
7.3.8 Repair phase 16
7.3.9 Destruction phase 17
7.4 Life cycle protection methods 17
7.4.1 Manufacturing 17
7.4.2 Post manufacturing phase 17
7.4.3 Commissioning (initial financial key loading) phase 17
7.4.4 Inactive Operational Phase 18
7.4.5 Active operational (use) phase 18
7.4.6 Decommissioning phase 18
7.4.7 Repair 19
7.4.8 Destruction 19
7.5 Accountability 19
7.6 Device management principles of audit and control 20

Annex A (informative) Evaluation methods 23

Bibliography 33